

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 11.07.96.

30 Priorité : 17.05.96 FR 9606382.

43 Date de la mise à disposition du public de la  
demande : 21.11.97 Bulletin 97/47.

56 Liste des documents cités dans le rapport de  
recherche préliminaire : *Se reporter à la fin du  
présent fascicule.*

60 Références à d'autres documents nationaux  
apparentés :

71 Demandeur(s) : GEMPLUS SOCIETE EN  
COMMANDITE PAR ACTIONS — FR.

72 Inventeur(s) : PROUST PHILIPPE, MOULINAS ANNE  
et HUET CEDRIC.

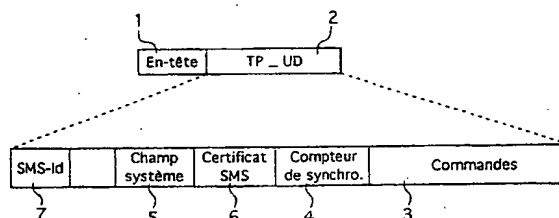
73 Titulaire(s) :

74 Mandataire : CABINET PATRICE VIDON.

54 MESSAGE AMELIORE ET PROCEDE CORRESPONDANT DE SYNCHRONISATION ET DE SECURISATION  
D'UN ECHANGE DE MESSAGES AMELIORES DANS UN SYSTEME DE RADIOCOMMUNICATION  
CELLULAIRE.

57 L'invention concerne une structure particulière de message amélioré, ainsi qu'un procédé de synchronisation et de sécurisation d'un échange de messages améliorés possédant cette structure. De façon classique, un message amélioré est transmis par un centre de service de messages vers un module d'identification d'abonné (ou module SIM) d'une station mobile. Le corps (2) de ce message amélioré contient notamment un premier champ (3) de stockage de commandes distantes appartenant à une application distante.

Selon l'invention, ce corps (2) contient également un second champ (4) de stockage de la valeur courante d'un compteur de synchronisation, destinée à être comparée à une valeur précédente du compteur de synchronisation, stockée dans le module SIM. Toujours selon l'invention, le corps (2) peut contenir un autre champ (6) de stockage d'un certificat, signature du corps, destiné à prouver l'authenticité du message amélioré et l'identité de son émetteur. Le message amélioré est accepté ou refusé par le module SIM en fonction de la cohérence de ces valeurs avec l'état interne du module SIM.



FR 2 748 880 - A1



**Message amélioré et procédé correspondant de synchronisation et de sécurisation d'un échange de messages améliorés dans un système de radiocommunication cellulaire.**

Le domaine de l'invention est celui des messages échangés dans les systèmes de radiocommunication cellulaire. Généralement, ces messages sont échangés entre un centre de service de messages et une pluralité de stations mobiles. Chaque station mobile est constituée d'un terminal coopérant avec une carte utilisateur à microprocesseur, appelée module d'identification d'abonné (ou module SIM, pour "Subscriber Identity Module" en langue anglaise).

Plus précisément, l'invention concerne une structure particulière de message amélioré, ainsi qu'un procédé de synchronisation et de sécurisation d'un échange de messages améliorés possédant cette structure.

Dans le domaine de la radiocommunication cellulaire, on connaît notamment, principalement en Europe, le standard GSM ("Groupe spécial Systèmes Mobiles publics de radiocommunication fonctionnant dans la bande des 900 Mhz").

L'invention s'applique notamment, mais non exclusivement, à un système selon ce standard GSM.

D'une façon générale, un terminal est un équipement physique utilisé par un usager du réseau pour accéder aux services de télécommunication offerts. Il existe différents types de terminaux, tels que notamment les portatifs, les portables ou encore les mobiles montés sur des véhicules.

Quand un terminal est utilisé par un usager, ce dernier doit connecter au terminal sa carte utilisateur (module SIM), qui se présente généralement sous la forme d'une carte à puce.

La carte utilisateur supporte une application principale téléphonique (par exemple l'application GSM) qui permet son fonctionnement, ainsi que celui du terminal auquel elle est connectée, dans le système de radiocommunication cellulaire. Notamment, la carte utilisateur procure au terminal auquel elle est connectée un identifiant unique d'abonné (ou identifiant IMSI, pour "International Mobile Subscriber Identity" en langue anglaise).

Pour cela, la carte utilisateur inclut des moyens d'exécution de commandes (par exemple,

un microprocesseur et une mémoire programme) et des moyens de mémorisation de données (par exemple une mémoire de données).

L'identifiant IMSI, ainsi que toutes les informations individuelles concernant l'abonné et destinées à être utilisées par le terminal, sont stockées dans les moyens de mémorisation de données du module SIM. Ceci permet à chaque terminal d'être utilisé avec n'importe quel module SIM.

Dans certains systèmes connus, et notamment dans un système GSM, il existe un service de messages (ou SMS, pour "Short Message Service" en langue anglaise) permettant l'envoi de messages (dits "messages courts" dans le cas du GSM) vers les stations mobiles. Ces messages sont émis par un centre de service de messages (ou SMS-C, pour "SMS-Center" en langue anglaise).

Lorsqu'une station mobile reçoit un message, elle le stocke dans les moyens de mémorisation de données de son module SIM. L'application principale téléphonique de chaque module SIM permet de traiter chaque message reçu.

A l'origine, l'unique fonction d'un message était de fournir une information à l'abonné, généralement via un écran d'affichage du terminal. Les messages, dits messages normaux, qui remplissent cette unique fonction ne contiennent donc que des données brutes.

Par la suite, on a imaginé un service de messages améliorés (ou ESMS, pour "Enhanced SMS" en langue anglaise), dans lequel deux types de messages peuvent être envoyés, à savoir les messages normaux précités et des messages améliorés pouvant contenir des commandes.

Ainsi, il a déjà été proposé de transmettre à un module SIM, via des messages améliorés, des commandes permettant de mettre à jour ou de reconfigurer ce module SIM à distance. En d'autres termes, des commandes encapsulées dans des messages améliorés permettent de modifier l'application principale téléphonique du module SIM. Ceci permet donc de reconfigurer le module SIM sans avoir à le ramener à un point de vente (et donc de faire exécuter au module SIM des commandes administratives alors qu'elle est en phase applicative).

On a également proposé que le module SIM serve de support à d'autres

applications que l'application principale téléphonique, telles que notamment des applications de location de voiture, de paiement ou encore de fidélité.

5 Du fait que les commandes appartenant à ces autres applications sont contenues dans des messages améliorés, et donc externes au module SIM, ces autres applications sont dites distantes ou OTA (pour "Over The Air" en langue anglaise). Par opposition, l'application principale téléphonique, dont les commandes sont contenues dans les moyens de mémorisation de données du module SIM, est dite locale. Les commandes sont également dites locales ou distantes, selon que l'application à laquelle elles appartiennent est elle-même locale ou distante.

10 Avec ces commandes distantes, on peut donc exécuter des applications distantes (location, paiement, reconfiguration de l'application principale téléphonique, ...).

15 Il est clair que ce récent concept d'application distante (ou application OTA) est très avantageux pour l'abonné. En effet, ce dernier peut maintenant effectuer de façon très simple, uniquement avec un terminal dans lequel est inséré son module SIM, de nombreuses opérations telles que par exemple la location d'une voiture ou le paiement d'un service.

20 En d'autres termes, on fait faire au module SIM autre chose (c'est-à-dire essentiellement plus de commandes) que ce qu'il est normalement capable de faire une fois qu'il est en phase applicative, c'est-à-dire une fois qu'il est inséré dans un téléphone mobile entre les mains d'un utilisateur.

Il découle de cette augmentation de la capacité de travail du module SIM des exigences de sécurité particulières. En effet, ce mécanisme, qui est en fait une porte d'entrée supplémentaire dans le module SIM, ne doit pas permettre à n'importe qui d'effectuer dans le module SIM des actions qui lui sont normalement interdites.

25 Parmi les exigences de sécurité particulières liées à l'utilisation des messages améliorés, on peut citer notamment la resynchronisation, l'unicité de chaque message, l'intégrité de chaque message et l'authenticité de l'entité émettrice.

30 Il convient en effet de pouvoir resynchroniser la source des messages et le module SIM en cas de problèmes de transmission sur le réseau. Du fait des aléas de transmission sur le canal des messages améliorés, ni l'acheminement d'un message amélioré ni l'ordre

d'acheminement de plusieurs messages améliorés ne peuvent en effet être garantis.

L'exigence d'unicité de chaque message permet d'éviter le rejeu d'un message, que ce soit de façon accidentelle (le canal de transmission suivi par le message amélioré est en effet tel qu'il peut arriver qu'un même message soit transmis plusieurs fois à un module SIM), ou bien intentionnelle (c'est-à-dire frauduleuse, le but étant alors de faire effectuer plusieurs fois de suite au module SIM la même séquence de commandes, comme par exemple celles qui permettraient de recrediter un compteur d'unités téléphoniques prépayées dans le module SIM).

L'exigence d'intégrité de chaque message permet d'éviter la corruption d'un message, que ce soit de façon accidentelle (due également au canal de transmission entre le centre de service de messages et la station mobile), ou bien intentionnelle (le but étant alors de modifier un message pour lui faire effectuer d'autres actions, plus sensibles, que celles prévues par la source du message).

L'exigence d'authenticité de l'entité émettrice permet de s'assurer que celle-ci est bien autorisée à envoyer des messages améliorés. En effet, ce mécanisme d'application distante doit être réservé à des émetteurs particuliers (tels que notamment les opérateurs et les fournisseurs de services).

Or, il apparaît que le récent concept d'application distante, tel qu'il est mis en oeuvre actuellement, ne répond pas à toutes ces exigences de sécurité particulières.

En effet, à ce jour, il a simplement été proposé d'introduire un total de contrôle (ou "checksum" en langue anglaise) dans chaque message amélioré, et d'effectuer une procédure de vérification de type présentation de code secret avant d'exécuter les commandes distantes contenus dans le message amélioré.

Il est clair que cette solution connue n'est pas satisfaisante car incomplète.

Tout d'abord, l'utilisation d'un total de contrôle, qui est une solution relativement basique, permet uniquement de s'assurer que la transmission s'est effectuée correctement.

Par ailleurs, la procédure de vérification de type présentation de code secret n'offre pas les garanties de sécurité suffisantes en cas d'interception d'un message amélioré. En effet, l'information d'identification ne variant pas d'un message à l'autre, il

est facile pour une personne non autorisée de rejouer un message, c'est-à-dire de faire passer pour authentique un message préalablement intercepté frauduleusement.

Enfin, cette solution connue ne vise aucunement à satisfaire aux autres exigences précitées, à savoir notamment celles concernant la resynchronisation et l'intégrité des messages.

L'invention a notamment pour objectif de pallier ces différents inconvénients de l'état de la technique.

Plus précisément, l'un des objectifs de la présente invention est de fournir un procédé de synchronisation et de sécurisation d'un échange de messages améliorés, ainsi qu'une structure correspondante de message amélioré, qui permettent de resynchroniser la source des messages et le module SIM en cas de problèmes de transmission sur le réseau.

L'invention a également pour objectif de fournir un tel procédé et une telle structure de message amélioré qui assurent l'unicité de chaque message amélioré transmis.

Un autre objectif de l'invention est de fournir un tel procédé et une telle structure de message amélioré qui assurent l'intégrité de chaque message amélioré transmis.

Un objectif complémentaire de l'invention est de fournir un tel procédé et une telle structure de message amélioré qui assurent l'authenticité de l'entité émettrice des messages améliorés.

Ces différents objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un message amélioré, du type transmis par un centre de service de messages vers une station mobile d'un système de radiocommunication cellulaire, ledit message amélioré comprenant un en-tête et un corps, ledit corps contenant notamment un premier champ de stockage de commandes distantes appartenant à une application distante de ladite station mobile,

ladite station mobile étant constituée d'un terminal coopérant avec un module d'identification d'abonné, ledit terminal comprenant des moyens de réception dudit message amélioré, ledit module d'identification d'abonné comprenant des moyens de stockage et de traitement dudit message amélioré reçu par le terminal, ledit module

d'identification d'abonné servant de support à ladite application distante et comprenant des moyens d'exécution desdites commandes distantes,

ledit message amélioré étant caractérisé en ce que ledit corps comprend également un second champ de stockage de la valeur courante d'un compteur de synchronisation,

5 ladite valeur courante du compteur de synchronisation étant destinée à être comparée à une valeur précédente du compteur de synchronisation stockée dans le module d'identification d'abonné, de façon que ledit message amélioré soit accepté ou refusé par le module d'identification d'abonné en fonction du résultat de la comparaison des valeurs courante et précédente du compteur de synchronisation, ladite valeur  
10 précédente étant mise à jour avec ladite valeur courante seulement après que le message amélioré a été accepté par le module d'identification d'abonné.

Ainsi, la synchronisation entre le centre de service de messages et le module d'identification d'abonné (ou module SIM) est basée sur l'utilisation d'un compteur partagé entre ces deux entités. Chaque message transmis au module SIM contient la  
15 valeur courante de ce compteur de synchronisation. Cette valeur courante est distincte pour chaque message. De son côté, le module SIM conserve la valeur précédente du compteur de synchronisation, qu'il compare à la valeur courante contenue dans chaque message, de façon à accepter ou refuser ce message.

En cas de problème lors de la transmission d'un message, le module SIM peut se  
20 resynchroniser avec la source de messages dès le message suivant puisque la valeur courante du compteur de synchronisation est contenue dans chaque message.

Dans le cas où le module SIM supporte plusieurs applications distantes, chacune de celles-ci peut être associée à un compteur de synchronisation distinct, le module SIM stockant alors les valeurs précédentes des différents compteurs.

25 Avantageusement, le corps dudit message amélioré comprend également un troisième champ de stockage d'une première information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation.

Ceci est particulièrement intéressant dans le cas où le module SIM supporte  
30 plusieurs applications distantes. En effet, dans ce cas, lorsqu'il reçoit un message, c'est

le contenu du troisième champ qui permet au module SIM de savoir quel compteur de synchronisation utiliser.

Dans un mode de réalisation particulier de l'invention, dans lequel lesdits moyens de mémorisation de données du module d'identification d'abonné possèdent une structure hiérarchique à au moins trois niveaux et comprennent au moins les trois types de fichiers suivants :

- fichier maître, ou répertoire principal ;
- fichier spécialisé, ou répertoire secondaire placé sous ledit fichier maître ;
- fichier élémentaire, placé sous un desdits fichiers spécialisés, dit fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent,

un fichier élémentaire système (EF SMS System), propre à ladite application distante, contenant une seconde information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation,

ledit message amélioré est caractérisé en ce que ladite première information de localisation contenue dans ledit troisième champ de stockage est un identificateur d'un fichier spécialisé ou d'un fichier maître auquel se rapporte ledit fichier élémentaire système selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

Ainsi, chaque message comporte un identificateur permettant au module SIM de retrouver le fichier élémentaire système auquel l'application distante émettrice de ce message est liée. Ce fichier élémentaire système comporte notamment la valeur précédente du compteur de synchronisation associé à cette application distante émettrice du message.

Préférentiellement, ledit corps comprend également un quatrième champ de stockage d'un cryptogramme, dit cryptogramme transmis, dont le calcul implique au moins en partie le contenu du second champ de stockage de la valeur courante du compteur de synchronisation,

ledit cryptogramme transmis étant destiné à être comparé à un autre cryptogramme, dit cryptogramme local, calculé par le module d'identification d'abonné, de façon que ledit message amélioré soit accepté par le module d'identification d'abonné



si les cryptogrammes transmis et local sont identiques, et refusé dans le cas contraire.

En d'autres termes, on combine l'utilisation d'un compteur de synchronisation et d'un cryptogramme. Ceci permet de sécuriser fortement l'échange de messages entre le centre de service de messages et le module SIM.

5 En effet, l'utilisation d'un cryptogramme permet au module SIM de s'assurer d'une part que la source émettrice du message est bien une source autorisée (on parle également de l'authenticité de l'entité émettrice), et d'autre part de l'intégrité du message.

De plus, il existe une synergie entre l'utilisation du compteur de synchronisation et celle du cryptogramme, du fait que le calcul de ce dernier implique la valeur courante  
10 du compteur.

Tout d'abord, la valeur courante du compteur étant différente pour chaque message, le même message ne peut pas être rejoué frauduleusement. En d'autres termes, on assure ainsi l'unicité de chaque message.

Par ailleurs, la valeur courante du compteur étant contenue dans le message, le  
15 module SIM sait quelle valeur courante a été utilisée pour le calcul du cryptogramme et peut donc calculer le cryptogramme de comparaison (cryptogramme local) sur les mêmes bases.

Enfin, la transmission de la valeur courante du compteur dans le message assure également qu'un message reçu peut être accepté, même si le ou les messages émis avant  
20 lui ne sont pas encore reçus (ou n'arrivent jamais).

Avantageusement, le calcul desdits cryptogrammes transmis et de vérification implique également au moins en partie le contenu du premier champ de stockage des commandes distantes.

Dans un mode de réalisation avantageux de l'invention, le calcul desdits  
25 cryptogrammes transmis et de vérification implique au moins tout le contenu du second champ de stockage de la valeur courante du compteur de synchronisation et tout le contenu du premier champ de stockage des commandes distantes. De cette façon, on augmente la qualité de la sécurisation.

De façon préférentielle, le calcul desdits cryptogrammes transmis et de vérification  
30 est effectué avec une fonction cryptographique appartenant au groupe comprenant :

- les fonctions cryptographiques à clé secrète ; et
- les fonctions cryptographiques à clé publique.

Ainsi, l'invention n'est pas limitée à l'utilisation d'un type particulier de fonction cryptographique.

5           Préférentiellement, ledit module d'identification d'abonné stockant, dans lesdits  
)   moyens de mémorisation de données du module d'identification d'abonné, une fonction  
)   cryptographique et une clé associée spécifiques à ladite application distante et permettant  
de calculer ledit cryptogramme local,

10           ledit message amélioré est caractérisé en ce que le corps dudit message amélioré  
comprend également un cinquième champ de stockage d'une troisième information de  
localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de  
données, de ladite fonction cryptographique et de ladite clé associée spécifiques à ladite  
application distante.

15           Ceci est particulièrement intéressant dans le cas où le module SIM supporte  
plusieurs applications distantes, chacune associée à un couple distinct (fonction  
cryptographique, clé), et où le module SIM stocke les différents couples associés à ces  
différentes applications. En effet, dans ce cas, lorsqu'il reçoit un message, c'est le  
contenu du cinquième champ qui permet au module SIM de savoir quel couple (fonction  
cryptographique, clé) utiliser.

20           Dans un mode de réalisation préférentiel de l'invention, ledit troisième champ  
constitue également ledit cinquième champ, ladite première information de localisation  
constituant également ladite troisième information de localisation.

25           De cette façon, le contenu du troisième champ permet au module SIM de savoir  
non seulement quel compteur de synchronisation utiliser, mais également quel couple  
(fonction cryptographique, clé).

          Avantageusement, ledit corps comprend également un sixième champ de stockage  
d'un total de contrôle, dit total de contrôle transmis, dont le calcul implique au moins en  
partie le contenu du premier champ de stockage des commandes distantes,

30           ledit total de contrôle transmis étant destiné à être comparé à un autre total de  
contrôle, dit total de contrôle local, calculé par le module d'identification d'abonné, de

façon que ledit message amélioré soit accepté par le module d'identification d'abonné si les totaux de contrôle transmis et local sont identiques, et refusé dans le cas contraire.

Cette utilisation d'un total de contrôle (ou "checksum" en langue anglaise) consitue un niveau supplémentaire de sécurisation. Ceci permet de rejeter rapidement, sans avoir à effectuer de calculs cryptographiques, un message qui aurait été modifié, par exemple de façon accidentelle.

De plus, dans le cas où l'on prévoit la possibilité de débrayer sous certaines conditions la vérification du cryptogramme et celle du compteur, le champ "total de contrôle" assure alors seul, mais avec un niveau garanti très relatif, qu'il n'y a pas eu corruption accidentelle ou intentionnelle du message. Il est clair cependant que cette possibilité doit être réservée à des configurations où la sécurité logique liée aux applications distantes limite les actions qui sont possibles dans le module SIM.

De façon avantageuse, ledit module d'identification d'abonné comprenant une ligne d'entrée/sortie sur laquelle il reçoit des commandes locales, appartenant à une application locale à ladite station mobile,

ledit message amélioré est caractérisé en ce que lesdites commandes distantes contenues dans ledit premier champ dudit message amélioré sont sensiblement identiques auxdites commandes locales reçues sur la ligne d'entrée/sortie.

De cette façon, le module SIM peut gérer les deux types de commandes, locales et distantes, sans qu'il soit nécessaire de dupliquer le code exécutable du module SIM (code généralement situé en mémoire ROM et/ou en mémoire EEPROM).

L'invention concerne également un procédé de synchronisation et de sécurisation d'un échange de messages améliorés entre un centre de service de messages et une station mobile d'un système de radiocommunication cellulaire, chaque message amélioré comprenant un en-tête et un corps, ledit corps contenant notamment un premier champ de stockage de commandes distantes appartenant à une application distante de ladite station mobile,

ladite station mobile étant constituée d'un terminal coopérant avec un module d'identification d'abonné, ledit terminal comprenant des moyens de réception dudit message amélioré, ledit module d'identification d'abonné comprenant des moyens de

stockage et de traitement dudit message amélioré reçu par le terminal, ledit module d'identification d'abonné servant de support à ladite application distante et comprenant des moyens d'exécution desdites commandes distantes,

ledit procédé étant caractérisé en ce qu'il comprend notamment les étapes suivantes :

- ledit centre de service de messages transmet à ladite station mobile un message amélioré dont le corps comprend également un second champ de stockage de la valeur courante d'un compteur de synchronisation ;
- le module d'identification d'abonné de la station mobile compare ladite valeur courante du compteur de synchronisation, contenue dans ledit message amélioré, avec une valeur précédente du compteur de synchronisation, stockée dans le module d'identification d'abonné ;
- le module d'identification d'abonné accepte ou refuse ledit message amélioré en fonction du résultat de la comparaison des valeurs courante et précédente du compteur de synchronisation ;
- si le message amélioré a été accepté, le module d'identification d'abonné met à jour ladite valeur précédente avec ladite valeur courante.

Préférentiellement, pour chaque nouveau message amélioré de ladite application distante transmis par ledit centre de service de messages, la valeur courante du compteur de synchronisation est incrémentée d'un pas prédéterminé,

et ledit message amélioré est accepté par le module d'identification d'abonné seulement si ladite valeur courante du compteur de synchronisation est supérieure à ladite valeur précédente.

En d'autres termes, pour éviter le rejeu d'un message, toute nouvelle valeur courante doit être supérieure à celle contenue dans le dernier message accepté (c'est-à-dire à la valeur précédente stockée dans le module SIM).

De façon préférentielle, ladite étape de mise à jour de la valeur précédente du compteur de synchronisation avec ladite valeur courante est effectuée seulement si la différence entre lesdites valeurs courante et précédente est inférieure à un pas d'incrément maximal prédéterminé.

De cette façon, on évite que le compteur soit trop rapidement bloqué à sa valeur maximale. En d'autres termes, on augmente la durée de vie du compteur, et on évite des attaques consistant à bloquer rapidement le module SIM en amenant le compteur à sa valeur maximale. En effet, lorsqu'il est ainsi bloqué, le compteur ne peut pas être remis à zéro par une application distante. Seule une procédure administrative peut permettre de le débloquer, ce qui engendre des coûts supplémentaires.

Avantageusement, ledit procédé comprend également l'étape suivante :

- lorsque ledit message amélioré est refusé par le module d'identification d'abonné, celui-ci renvoie au centre de service de messages un message amélioré contenant un code d'erreur spécifique, permettant au centre de service de messages de savoir que ledit message amélioré qu'il a précédemment émis a été refusé pour un problème de synchronisation de compteur.

Ceci est notamment le cas lorsque deux messages successifs, par exemple, de valeurs courantes de compteur  $N$  et  $N+1$  respectivement, ne sont pas reçus dans leur ordre d'émission. En effet, si le premier message reçu est accepté, le second message est quant à lui refusé (comme expliqué ci-dessous) et l'entité émettrice peut alors avantageusement être prévenue de la cause de ce refus, à savoir un problème de synchronisation.

On comprend en effet que lorsque le module SIM reçoit le premier message (de valeur  $N+1$ ), la valeur précédente qu'il stocke est  $N-1$ . Par conséquent, la valeur courante du premier message, égale à  $N+1$ , est supérieure à cette valeur  $N-1$ . Ensuite, la valeur précédente est mise à jour avec la valeur courante du premier message reçu, et lorsque le module SIM reçoit le second message, la valeur précédente qu'il stocke est donc  $N+1$ . Par conséquent, la valeur courante du second message, égale à  $N$ , est inférieure à cette valeur précédente  $N+1$ , ce qui justifie le refus de ce second message pour problème de synchronisation.

De façon avantageuse, le corps dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un troisième champ de stockage d'une première information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de

ladite valeur précédente du compteur de synchronisation,

ladite étape de comparaison par le module d'identification d'abonné des valeurs courante et précédente du compteur de synchronisation étant précédée des étapes suivantes :

- 5        -        le module d'identification d'abonné lit ladite première information de localisation contenue dans le troisième champ dudit message amélioré ;
- le module d'identification d'abonné en déduit l'emplacement de stockage de la valeur précédente du compteur de synchronisation ;
- le module d'identification d'abonné lit, audit emplacement de stockage, la valeur
- 10        précédente du compteur de synchronisation.

Dans un mode de réalisation préférentiel de l'invention, le corps dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un quatrième champ de stockage d'un cryptogramme, dit cryptogramme transmis, calculé en utilisant au moins en partie le contenu du second champ de stockage

15        de la valeur courante du compteur de synchronisation,

et ledit procédé comprend également les étapes suivantes :

- le module d'identification d'abonné calcule un cryptogramme local, en utilisant au moins en partie le contenu du second champ dudit message amélioré ;
- le module d'identification d'abonné compare ledit cryptogramme transmis et ledit
- 20        cryptogramme local, de façon que ledit message amélioré soit accepté si les cryptogrammes transmis et local sont identiques, et refusé dans le cas contraire.

Avantageusement, ledit module d'identification d'abonné stockant, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, une fonction cryptographique et une clé associée spécifiques à ladite application distante permettant de

25        calculer ledit cryptogramme local,

ledit procédé est caractérisé en ce que le corps dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un cinquième champ de stockage d'une troisième information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données, de ladite fonction

30        cryptographique et de ladite clé associée,

et en ce que ladite étape de calcul par le module d'identification d'abonné dudit cryptogramme local comprend les étapes suivantes :

- le module d'identification d'abonné lit ladite troisième information de localisation contenue dans le cinquième champ dudit message amélioré ;
- le module d'identification d'abonné en déduit l'emplacement de stockage de ladite fonction cryptographique et de ladite clé associée ;
- le module d'identification d'abonné calcule ledit cryptogramme local, en utilisant ladite fonction cryptographique, ladite clé associée et au moins une partie du contenu du second champ dudit message amélioré.

Dans un mode de réalisation avantageux de l'invention, dans lequel lesdits moyens de mémorisation de données du module d'identification d'abonné possèdent une structure hiérarchique à au moins trois niveaux et comprennent au moins les trois types de fichiers suivants :

- fichier maître, ou répertoire principal ;
- fichier spécialisé, ou répertoire secondaire placé sous ledit fichier maître ;
- fichier élémentaire, placé sous un desdits fichiers spécialisés, dit fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent,

ledit procédé est caractérisé en ce qu'un fichier élémentaire système (EF SMS System), propre à ladite application distante, contient une seconde information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation, de ladite fonction cryptographique et de ladite clé associée,

en ce que ledit troisième champ constitue également ledit cinquième champ, ladite première information de localisation constituant également ladite troisième information de localisation,

et en ce que ladite première information de localisation contenue dans ledit troisième champ de stockage est un identificateur d'un fichier spécialisé (DF) ou d'un fichier maître (MF) auquel se rapporte ledit fichier élémentaire système (EF SMS System) selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

Avantageusement, le corps dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un sixième champ de stockage d'un total de contrôle, dit total de contrôle transmis, dont le calcul implique au moins en partie le contenu du premier champ de stockage des commandes distantes,

5           ledit procédé comprenant également les étapes suivantes :

- ) le module d'identification d'abonné calcule un total de contrôle local, en utilisant  
  ) au moins en partie le contenu du premier champ dudit message amélioré ;
  - le module d'identification d'abonné compare ledit total de contrôle transmis et  
  ledit total de contrôle local, de façon que ledit message amélioré soit accepté si les
- 10           totaux de contrôle transmis et local sont identiques, et refusé dans le cas contraire.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation préférentiel de l'invention, donné à titre d'exemple indicatif et non limitatif, et des dessins annexés, dans lesquels :

- la figure 1 présente un mode de réalisation particulier de la structure d'un  
15       message amélioré selon l'invention ;
- les figures 2 à 4 présentent chacune un exemple d'échange de messages  
     améliorés sécurisé selon le procédé de l'invention ;
- la figure 5 présente un exemple de calcul d'un cryptogramme utilisé dans  
     le procédé de l'invention ;
- 20   -   la figure 6 présente un organigramme simplifié d'un mode de réalisation  
     particulier du procédé de l'invention ; et
- les figures 7 à 9 présentent chacune, de façon plus détaillée, une des  
     étapes apparaissant sur l'organigramme de la figure 6.

25           L'invention concerne donc une structure particulière de message amélioré, ainsi  
     qu'un procédé de synchronisation et de sécurisation d'un échange de messages améliorés  
     possédant cette structure.

30           Dans le mode de réalisation particulier décrit ci-dessous, uniquement à titre  
     d'exemple indicatif et non limitatif, le système de radiocommunication cellulaire est du  
     type GSM et met en oeuvre un service de messages courts améliorés (ou ESMS, pour  
     "Enhanced Short Message Service" en langue anglaise).



Il est clair toutefois que l'invention n'est pas limitée à un système de type GSM, mais concerne plus généralement tous les systèmes de radiocommunication cellulaire proposant un service de messages améliorés.

De façon classique, dans le cas du GSM, les messages courts améliorés sont échangés entre un centre de service de messages courts (SMS-C) et une ou plusieurs stations mobiles (MS) parmi une pluralité. Chaque station mobile est constituée d'un terminal coopérant avec un module d'identification d'abonné (module SIM). Le terminal comprend des moyens de réception d'un message amélioré. Le module SIM comprend des moyens de stockage et de traitement du message amélioré reçu par le terminal. Chaque message amélioré contient des commandes distantes appartenant à une application distante du module SIM. Le module SIM sert de support à cette application distante (et éventuellement à d'autres) et comprend des moyens d'exécution de ces commandes distantes.

La figure 1 présente un mode de réalisation particulier de la structure d'un message amélioré selon l'invention.

De façon classique, le message amélioré comprend un en-tête 1 et un corps 2 (ou TP-UD, pour "Transfer layer Protocol - User Data" en langue anglaise). Le corps 2 contient notamment un champ "Commandes" 3, dans lequel sont stockées des commandes distantes.

Selon l'invention, il s'agit par exemple de commandes classiques (opérationnelles ou administratives), définies dans les normes GSM 11.11, ISO 78.16-4 ou encore EN 726-3, telles que SELECT, UPDATE BINARY, UPDATE RECORD, SEEK, CREATE FILE, CREATE RECORD, EXTEND, etc. En d'autres termes, le format de ces commandes distantes est identique à celui des commandes locales que le module SIM reçoit normalement sur sa ligne d'entrée/sortie. Le module SIM peut donc traiter les commandes distantes de la même façon que des commandes locales.

Dans le mode de réalisation particulier présenté sur la figure 1, le corps 2 du message amélioré de l'invention comprend plusieurs autres champs, à savoir notamment un champ "Compteur de synchronisation" 4, un champ "Système" 5, un champ "Certificat SMS" 6 et un champ "SMS-Id" 7.

On présente maintenant, de façon détaillée, le contenu de chacun de ces autres champs 4 à 7 du corps 2 du message amélioré.

5 Le champ "Compteur de synchronisation" 4 contient la valeur courante d'un compteur de synchronisation. Comme expliqué plus précisément par la suite, en relation avec les figures 2 à 4, 6 et 8, cette valeur courante du compteur de synchronisation est destinée à être comparée à une valeur précédente de ce même compteur de synchronisation, qui est stockée dans les moyens de mémorisation de données du module SIM. En fonction du résultat de cette comparaison, le message amélioré est soit accepté soit refusé par le module SIM.

10 Le champ "Système" 5 contient une information de localisation, dans les moyens de mémorisation de données du module SIM, d'un fichier système contenant lui-même soit directement des éléments propres à l'application distante émettrice du message, soit une autre information de localisation, dans les moyens de mémorisation de données du module SIM, de ces éléments.

15 Par éléments propres à l'application distante émettrice, on entend notamment la valeur précédente du compteur de synchronisation ainsi qu'une fonction cryptographique et sa clé associée (ces deux derniers éléments permettant de calculer un cryptogramme "local" destiné à être comparé à un cryptogramme "transmis" contenu dans le champ "Certificat SMS" 6).

20 Il est connu de prévoir, pour les moyens de mémorisation de données du module SIM, une structure hiérarchique à au moins trois niveaux, avec les trois types de fichiers suivants :

- fichier maître (MF), ou répertoire principal ;
- fichier spécialisé (DF), ou répertoire secondaire placé sous le fichier maître ;
- 25 - fichier élémentaire (EF), placé sous un des fichiers spécialisés, dit fichier spécialisé parent, ou directement sous le fichier maître, dit fichier maître parent.

Dans le cas d'une telle structure hiérarchique, le fichier système précité de l'invention est par exemple un fichier élémentaire système (EF SMS System). L'information de localisation contenue dans le champ "Système" 5 est alors un  
30 identificateur ("DF entrée") d'un fichier spécialisé (DF) ou d'un fichier maître (MF)

auquel se rapporte le fichier élémentaire système (EF SMS System) selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

Le module SIM met par exemple en oeuvre un mécanisme de recherche en amont (du type "backtracking"), consistant :

- 5                   - à rechercher un fichier élémentaire système tout d'abord sous le fichier spécialisé ou le fichier maître courant (c'est-à-dire celui indiqué par l'identificateur "DF entrée"),
- puis, si aucun fichier élémentaire système n'existe sous le fichier spécialisé ou le fichier maître courant et si l'identificateur "DF entrée"
- 10                n'indique pas le fichier maître, à rechercher un fichier élémentaire système directement sous le fichier maître.

Ainsi, le module SIM lit dans le message amélioré l'identificateur "DF entrée" contenu dans le champ "Système" 5. A partir de cet identificateur "DF entrée", il retrouve le fichier élémentaire système auquel est liée l'application distante émettrice du message.

15                Dans ce fichier élémentaire système, le module SIM lit par exemple :

- directement la valeur courante du compteur de synchronisation ; et
- l'identificateur d'un fichier spécialisé sous lequel se trouve un fichier EF key\_op contenant le couple (fonction cryptographique, clé associée) lié à l'application distante émettrice du message.

20                Le champ "Certificat SMS" 6 contient un cryptogramme (appelé "cryptogramme transmis" dans la suite de la description). Comme expliqué plus précisément par la suite, en relation avec les figures 6 et 9, ce cryptogramme transmis est destiné à être comparé à un cryptogramme local, qui lui est calculé par le module SIM. En fonction du résultat de cette comparaison, le message amélioré est soit accepté soit refusé par le module SIM.

25                On présente maintenant un mode de réalisation particulier du calcul du cryptogramme transmis SMS-Cert (ce calcul est bien sûr identique à celui du cryptogramme local). On a la relation :

SMS-Cert = 4 octets les moins significatifs de [MAC\_Algalgo\_id (K\_appli, SMS\_data)], où

- "Algalgo\_id" est l'algorithme associé à l'application distante (la localisation de cet
- 30                algorithme est possible grâce au fichier élémentaire système (EF SMS System)

dont dépend cette application distante) ;

- $K_{\text{appli}}$  est la clé secrète (ou publique) associée à l'algorithme  $\text{Alg}_{\text{algo\_id}}$  ;
- "SMS\_data" = Sync | Message applicatif, où :
  - \* "I" symbolise l'opérateur de concaténation ;
  - \* "Sync" est la valeur (courante, pour le calcul du cryptogramme transmis) du compteur de synchronisation ;
  - \* "Message applicatif" est le contenu du champ "Commandes" 3 (dans lequel sont stockées les commandes distantes) ;
- $\text{MAC}_{\text{Alg}_{\text{algo\_id}}}$  est une fonction basée sur l'algorithme  $\text{Alg}_{\text{algo\_id}}$ , qui réalise un calcul du type "MAC" (pour "Message Authentication Code" en anglo-saxon) sur la concaténation SMS\_data, en utilisant la clé  $K_{\text{appli}}$ .

La figure 5 présente un exemple de calcul du cryptogramme transmis SMS-Cert, dans le cas où l'algorithme  $\text{Alg}_{\text{algo\_id}}$  est le MoU A3A8. Il est clair cependant que l'algorithme A3A8 n'est qu'un exemple d'implémentation, et que d'autres algorithmes peuvent être utilisés. Notamment une implémentation plus généraliste consiste à spécifier, pour une application particulière, l'algorithme à utiliser (au moyen d'un identifiant d'algorithme).

La concaténation SMS\_data est divisée en  $n$  blocs  $B_1, B_2, \dots, B_{n-1}, B_n$ , avec  $n \leq 9$ . Les blocs  $B_1$  à  $B_n$  comprennent par exemple 16 octets. Si la longueur de la concaténation SMS\_data ne permet pas d'obtenir un dernier bloc  $B_n$  comprenant 16 octets, ce dernier bloc est justifié à gauche et complété sur la droite avec des octets de valeur 0, de façon à construire un bloc comprenant 16 octets appelé  $B'_n$ . Ces blocs sont impliqués dans les calculs suivants :

$$I_1 = \text{A3A8}(K_{\text{appli}}, B_1)$$

$$R_2 = \text{XOR}(I_1, B_2)$$

$$I_2 = \text{A3A8}(K_{\text{appli}}, R_2)$$

...

$$R_{n-1} = \text{XOR}(I_{n-2}, B_{n-1})$$

$$I_{n-1} = \text{A3A8}(K_{\text{appli}}, R_{n-1})$$

$$R_n = \text{XOR}(I_{n-1}, B'_n)$$

$$I_n = A3A8(K_{\text{appli}}, R_n)$$

$I_n$  est le résultat de la fonction MAC\_A3A8. XOR est l'opérateur réalisant un "OU-exclusif" bit-par-bit entre deux chaînes de 16 octets.

Le champ "SMS-Id" 7 contient un total de contrôle (appelé "total de contrôle transmis" dans la suite de la description). Comme expliqué plus précisément par la suite, en relation avec les figures 6 et 7, ce total de contrôle transmis est destiné à être comparé à un total de contrôle local, qui lui est calculé par le module SIM. En fonction du résultat de cette comparaison, le message amélioré est soit accepté soit refusé par le module SIM.

On présente maintenant un mode de réalisation particulier du calcul du total de contrôle transmis SMS\_Id (ce calcul est bien sûr identique à celui du total de contrôle local). On a la relation :  $\text{SMS\_Id} = \text{NON}(\sum \text{octets du champ "Commandes" 3})$ .

La figure 6 présente un organigramme simplifié d'un mode de réalisation particulier du procédé de l'invention de synchronisation et de sécurisation d'un échange de messages améliorés possédant la structure de la figure 1.

Dans ce mode de réalisation particulier, le procédé de l'invention comprend notamment les étapes suivantes :

- le centre de service de messages transmet (61) un message amélioré au module SIM de la station mobile ;
- le module SIM vérifie (62) le total de contrôle transmis, qui est contenu dans le champ "SMS-Id" 7 du message amélioré ;
- si (63) le résultat de la vérification du total de contrôle transmis n'est pas correct, le message amélioré est refusé par le module SIM, sinon (64) le module SIM vérifie (65) la valeur courante du compteur de synchronisation, qui est contenue dans le champ "Compteur de synchronisation" 4 ;
- si (66) le résultat de la vérification de la valeur courante du compteur de synchronisation n'est pas correct, le message amélioré est refusé par le module SIM, sinon (67) le module SIM met immédiatement à jour la valeur précédente du compteur avec la valeur courante, et ce avant toute autre vérification. Puis il vérifie (68) le cryptogramme transmis, qui est

contenu dans le champ "Certificat SMS" 6 ;

- si (69) le résultat de la vérification du cryptogramme transmis n'est pas correct, le message amélioré est refusé par le module SIM, sinon (610) le module SIM exécute (611) les commandes distantes contenues dans le champ "Commandes" 3.

Comme présenté plus en détail sur la figure 7, l'étape (62) de vérification du total de contrôle transmis comprend elle-même les étapes suivantes :

- le module SIM lit (71), dans le champ "SMS-Id" 7 du message amélioré, le total de contrôle transmis ;
- le module SIM calcule (72) un total de contrôle local, selon la même règle de calcul que celle utilisée pour calculer le total de contrôle transmis ;
- le module SIM compare (73) le total de contrôle transmis et le total de contrôle local.

Ainsi, à ce premier niveau de vérification, le message amélioré est accepté (64) si les totaux de contrôle transmis et local sont identiques, et refusé (63) dans le cas contraire.

Comme présenté plus en détail sur la figure 8, l'étape (65) de vérification de la valeur courante du compteur de synchronisation comprend elle-même les différentes étapes suivantes :

- le module SIM lit (81), dans le champ "Compteur de synchronisation" 4, la valeur courante du compteur de synchronisation ;
- le module SIM lit (82), dans le champ "Système" 5 du message amélioré, une information de localisation d'un fichier système (EF SMS System). Comme déjà expliqué ci-dessus, cette information de localisation est par exemple l'identificateur "DF entrée" d'un fichier spécialisé (DF) ou d'un fichier maître (MF) auquel se rapporte ce fichier élémentaire système (EF SMS System) ;
- le module SIM en déduit (83) l'emplacement, dans les moyens de mémorisation de données du module SIM, du fichier système (EF SMS System) qui contient notamment la valeur précédente du compteur de synchronisation ;
- le module SIM lit (84), dans le fichier système (EF SMS System), la valeur

précédente du compteur de synchronisation ;

- le module SIM compare (85) la valeur courante du compteur de synchronisation avec la valeur précédente stockée dans le module SIM ;
- à ce second niveau de vérification, le message amélioré est accepté par le module SIM si (67) la valeur courante est strictement supérieure à la valeur précédente du compteur de synchronisation. Le module SIM peut alors mettre à jour (86) la valeur précédente avec la valeur courante ;
- si (66) la valeur courante est inférieure ou égale à la précédente du compteur de synchronisation, le message amélioré est refusé par le module SIM. Le module SIM peut alors renvoyer (87) au centre de service de messages un message amélioré contenant un code d'erreur spécifique, permettant au centre de service de messages de savoir que le message amélioré qu'il a précédemment émis a été refusé pour un problème de synchronisation de compteur.

On peut par exemple décider que pour chaque nouveau message amélioré transmis par le centre de service de messages, la valeur courante du compteur de synchronisation est incrémentée d'un pas prédéterminé (par exemple égal à 1). Un message amélioré n'est alors accepté par le module SIM que si la valeur courante du compteur de synchronisation que contient ce message amélioré est supérieure à la valeur précédente stockée par le module SIM.

On peut également prévoir que l'étape 86 de mise à jour de la valeur précédente du compteur de synchronisation avec la valeur courante n'est effectuée que si la différence entre les valeurs courante et précédente du compteur de synchronisation est inférieure à un pas d'incrément maximal prédéterminé.

Les figures 2 à 4 présentent différents exemples d'échange de messages améliorés sécurisé selon le procédé de l'invention. Sur chaque figure, on représente l'évolution de la valeur courante du compteur, notée E\_Sync (dans le "monde extérieur", sur la gauche) et celle de la valeur stockée, notée S\_Sync (dans le module SIM, sur la droite). Chaque flèche représente un message.

Dans le premier cas (cf fig.2), la synchronisation et la transmission du message amélioré sont correctes. On a :  $E\_Sync (= 1) > S\_Sync (= 0)$ . La valeur précédente est

mise à jour à 1 et les commandes distantes sont exécutées.

Dans le second cas (cf fig.3), il y a un problème lors de la transmission du message amélioré. Le module SIM ne répond pas. Par contre, la seconde tentative de transmission se déroule sans problème. Finalement, on a :  $E\_Sync (= 3) > S\_Sync (= 1)$ .

5 La valeur précédente est mise à jour à 3 et les commandes distantes sont exécutées.

Dans le troisième cas (cf fig.4), il y a un problème de synchronisation au départ. En effet, on a :  $E\_Sync (= 1) < S\_Sync (= 5)$ . Plusieurs messages améliorés comprenant des valeurs courantes successivement incrémentées sont envoyés jusqu'à ce que le centre de service de messages soit à nouveau synchronisé avec le module SIM. Ceci est le cas  
10 lorsque l'on a :  $E\_Sync (= 6) > S\_Sync (= 5)$ . La valeur précédente peut alors être mise à jour à 6 et les commandes distantes sont exécutées.

Comme présenté plus en détail sur la figure 9, l'étape (68) de vérification du cryptogramme transmis comprend elle-même les différentes étapes suivantes :

- le module SIM lit (91), dans le champ "Certificat SMS" 6, la valeur courante du  
15 compteur de synchronisation ;
- le module SIM calcule (92) un cryptogramme local, selon la même règle de calcul que celle utilisée pour calculer le cryptogramme transmis ;
- le module SIM compare (93) le cryptogramme transmis et le cryptogramme local.

Ainsi, à ce troisième niveau de vérification, le message amélioré est accepté (610)  
20 si les cryptogrammes transmis et local sont identiques, et refusé (69) dans le cas contraire.

Sur la figure 9, on a également présenté de façon plus détaillée l'étape 92 de calcul du cryptogramme local, qui comprend elle-même les étapes suivantes :

- le module SIM lit (94), dans le champ "Système" 5 du message amélioré, une  
25 information de localisation d'un fichier système (EF SMS System) ;
- le module SIM en déduit (95) l'emplacement, dans les moyens de mémorisation de données du module SIM, du fichier système (EF SMS System). Ce fichier système contient lui-même une autre information de localisation permettant au module SIM de retrouver la fonction cryptographique et sa clé associée, qui sont  
30 liées à l'application distante émettrice du message amélioré ;



- le module SIM calcule (96) le cryptogramme local, en utilisant la fonction cryptographique et sa clé associée, comme expliqué précédemment.

Il est à noter que l'étape référencée 94 et le début de celle référencée 95 sont en réalité déjà effectués, comme expliqué précédemment, pour retrouver la valeur précédente du compteur de synchronisation (qui quant à elle est directement stockée dans le fichier système (EF SMS System)).

Il est clair que de nombreux autres modes de réalisation de l'invention peuvent être envisagés.

On peut notamment prévoir deux fichiers système distincts pour retrouver d'une part la valeur précédente du compteur de synchronisation et d'autre part la fonction cryptographique et sa clé associée. Dans ce cas, on a deux champs "Système" du type de celui référencé 5.

On peut également prévoir que la fonction cryptographique soit du type à clé publique.

Enfin, il est à noter que l'étape 62 de vérification du total de contrôle, comme celle 68 de vérification du cryptogramme transmis, peut éventuellement être omise.

## REVENDICATIONS

1. Message amélioré, du type transmis par un centre de service de messages (C-SMS) vers une station mobile (MS) d'un système de radiocommunication cellulaire, ledit message amélioré comprenant un en-tête (1) et un corps (2), ledit corps (2) contenant  
5 notamment un premier champ (3) de stockage de commandes distantes appartenant à une application distante de ladite station mobile, )

) ladite station mobile étant constituée d'un terminal coopérant avec un module d'identification d'abonné, ledit terminal comprenant des moyens de réception dudit message amélioré, ledit module d'identification d'abonné comprenant des moyens de  
10 stockage et de traitement dudit message amélioré reçu par le terminal, ledit module d'identification d'abonné servant de support à ladite application distante et comprenant des moyens d'exécution desdites commandes distantes,

ledit message amélioré étant caractérisé en ce que ledit corps (2) comprend également un second champ (4) de stockage de la valeur courante d'un compteur de  
15 synchronisation,

ladite valeur courante du compteur de synchronisation étant destinée à être comparée à une valeur précédente du compteur de synchronisation stockée dans le module d'identification d'abonné, de façon que ledit message amélioré soit accepté ou refusé par le module d'identification d'abonné en fonction du résultat de la comparaison  
20 des valeurs courante et précédente du compteur de synchronisation, ladite valeur précédente étant mise à jour avec ladite valeur courante seulement après que le message amélioré a été accepté par le module d'identification d'abonné.

2. Message amélioré selon la revendication 1, caractérisé en ce que le corps (2) dudit message amélioré comprend également un troisième champ (5) de stockage d'une  
25 première information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation.

3. Message amélioré selon la revendication 2, lesdits moyens de mémorisation de données du module d'identification d'abonné possédant une structure hiérarchique à au  
30 moins trois niveaux et comprenant au moins les trois types de fichiers suivants :

- fichier maître (MF), ou répertoire principal ;
  - fichier spécialisé (DF), ou répertoire secondaire placé sous ledit fichier maître ;
  - fichier élémentaire (EF), placé sous un desdits fichiers spécialisés, dit fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent,
- 5 un fichier élémentaire système (EF SMS System), propre à ladite application distante, contenant une seconde information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation,

10 ledit message amélioré étant caractérisé en ce que ladite première information de localisation contenue dans ledit troisième champ (5) de stockage est un identificateur d'un fichier spécialisé (DF) ou d'un fichier maître (MF) auquel se rapporte ledit fichier élémentaire système (EF SMS System) selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

15 4. Message amélioré selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit corps comprend également un quatrième champ (6) de stockage d'un cryptogramme, dit cryptogramme transmis, dont le calcul implique au moins en partie le contenu du second champ de stockage de la valeur courante du compteur de synchronisation,

20 ledit cryptogramme transmis étant destiné à être comparé à un autre cryptogramme, dit cryptogramme local, calculé par le module d'identification d'abonné, de façon que ledit message amélioré soit accepté par le module d'identification d'abonné si les cryptogrammes transmis et local sont identiques, et refusé dans le cas contraire.

25 5. Message amélioré selon la revendication 4, caractérisé en ce que le calcul desdits cryptogrammes transmis et de vérification implique également au moins en partie le contenu du premier champ (3) de stockage des commandes distantes.

6. Message amélioré selon la revendication 5, caractérisé en ce que le calcul desdits cryptogrammes transmis et local implique au moins tout le contenu du second champ (4) de stockage de la valeur courante du compteur de synchronisation et tout le contenu du premier champ (3) de stockage des commandes distantes.

30 7. Message amélioré selon l'une quelconque des revendications 4 à 6, caractérisé en

ce que le calcul desdits cryptogrammes transmis et local est effectué avec une fonction cryptographique appartenant au groupe comprenant :

- les fonctions cryptographiques à clé secrète ; et
- les fonctions cryptographiques à clé publique.

5        8.        Message amélioré selon l'une quelconque des revendications 1 à 7, ledit module d'identification d'abonné stockant, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, une fonction cryptographique et une clé associée spécifiques à ladite application distante et permettant de calculer ledit cryptogramme local,

10            ledit message amélioré étant caractérisé en ce que le corps dudit message amélioré comprend également un cinquième champ (5) de stockage d'une troisième information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données, de ladite fonction cryptographique et de ladite clé associée spécifiques à ladite application distante.

15        9.        Message amélioré selon les revendications 2 et 8, caractérisé en ce que ledit troisième champ (5) constitue également ledit cinquième champ, ladite première information de localisation constituant également ladite troisième information de localisation.

20        10.       Message amélioré selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ledit corps (2) comprend également un sixième champ (7) de stockage d'un total de contrôle, dit total de contrôle transmis, dont le calcul implique au moins en partie le contenu du premier champ (3) de stockage des commandes distantes,

25            ledit total de contrôle transmis étant destiné à être comparé à un autre total de contrôle, dit total de contrôle local, calculé par le module d'identification d'abonné, de façon que ledit message amélioré soit accepté par le module d'identification d'abonné si les totaux de contrôle transmis et local sont identiques, et refusé dans le cas contraire.

3        11.       Message amélioré selon l'une quelconque des revendications 1 à 10, ledit module d'identification d'abonné comprenant une ligne d'entrée/sortie sur laquelle il reçoit des commandes locales, appartenant à une application locale à ladite station mobile,

30            caractérisé en ce que lesdites commandes distantes contenues dans ledit premier champ (3) dudit message amélioré sont sensiblement identiques auxdites commandes

locales reçues sur la ligne d'entrée/sortie.

12. Procédé de synchronisation et de sécurisation d'un échange de messages améliorés entre un centre de service de messages (C-SMS) et une station mobile (MS) d'un système de radiocommunication cellulaire, chaque message amélioré comprenant un en-tête (1) et un corps (2), ledit corps (2) contenant notamment un premier champ (3) de stockage de commandes distantes appartenant à une application distante de ladite station mobile.

ladite station mobile étant constituée d'un terminal coopérant avec un module d'identification d'abonné, ledit terminal comprenant des moyens de réception dudit message amélioré, ledit module d'identification d'abonné comprenant des moyens de stockage et de traitement dudit message amélioré reçu par le terminal, ledit module d'identification d'abonné servant de support à ladite application distante et comprenant des moyens d'exécution desdites commandes distantes,

ledit procédé étant caractérisé en ce qu'il comprend notamment les étapes suivantes :

- ledit centre de service de messages transmet (61) à ladite station mobile un message amélioré dont le corps comprend également un second champ (4) de stockage de la valeur courante d'un compteur de synchronisation ;
- le module d'identification d'abonné de la station mobile compare (65 ; 85) ladite valeur courante du compteur de synchronisation, contenue dans ledit message amélioré, avec une valeur précédente du compteur de synchronisation, stockée dans le module d'identification d'abonné ;
- le module d'identification d'abonné accepte (67) ou refuse (66) ledit message amélioré en fonction du résultat de la comparaison des valeurs courante et précédente du compteur de synchronisation ;
- si le message amélioré a été accepté, le module d'identification d'abonné met à jour (86) ladite valeur précédente avec ladite valeur courante.

13. Procédé selon la revendication 12, caractérisé en ce que, pour chaque nouveau message amélioré de ladite application distante transmis par ledit centre de service de messages, la valeur courante du compteur de synchronisation est incrémentée d'un pas

prédéterminé,

et en ce que ledit message amélioré est accepté par le module d'identification d'abonné seulement si ladite valeur courante du compteur de synchronisation est supérieure à ladite valeur précédente.

5 14. Procédé selon l'une quelconque des revendications 12 et 13, caractérisé en ce que ladite étape de mise à jour de la valeur précédente du compteur de synchronisation avec ladite valeur courante est effectuée seulement si la différence entre lesdites valeurs courante et précédente est inférieure à un pas d'incrément maximal prédéterminé.

10 15. Procédé selon l'une quelconque des revendications 12 à 14, caractérisé en ce qu'il comprend également l'étape suivante :

- lorsque ledit message amélioré est refusé (66) par le module d'identification d'abonné, celui-ci renvoie (87) au centre de service de messages un message amélioré contenant un code d'erreur spécifique, permettant au centre de service de messages de savoir que ledit message amélioré qu'il a précédemment émis a été refusé pour un problème de synchronisation de compteur.

15 16. Procédé selon l'une quelconque des revendications 12 à 15, caractérisé en ce que le corps (2) dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un troisième champ (5) de stockage d'une première information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation,

20 et en ce que ladite étape (85) de comparaison par le module d'identification d'abonné des valeurs courante et précédente du compteur de synchronisation est précédée des étapes suivantes :

- 25 - le module d'identification d'abonné lit (82) ladite première information de localisation contenue dans le troisième champ dudit message amélioré ;
- le module d'identification d'abonné en déduit (83) l'emplacement de stockage de la valeur précédente du compteur de synchronisation ;
- 30 - le module d'identification d'abonné lit (84), audit emplacement de stockage, la valeur précédente du compteur de synchronisation.

17. Procédé selon l'une quelconque des revendications 12 à 16, caractérisé en ce que le corps (2) dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un quatrième champ (6) de stockage d'un cryptogramme, dit cryptogramme transmis, calculé en utilisant au moins en partie le contenu du second champ (4) de stockage de la valeur courante du compteur de synchronisation,

et en ce que ledit procédé comprend également les étapes suivantes :

- le module d'identification d'abonné calcule (92) un cryptogramme local, en utilisant au moins en partie le contenu du second champ (4) dudit message amélioré ;
- le module d'identification d'abonné compare (93) ledit cryptogramme transmis et ledit cryptogramme local, de façon que ledit message amélioré soit accepté si les cryptogrammes transmis et local sont identiques, et refusé dans le cas contraire.

18. Procédé selon l'une quelconque des revendications 12 à 17, ledit module d'identification d'abonné stockant, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, une fonction cryptographique et une clé associée spécifiques à ladite application distante permettant de calculer ledit cryptogramme local,

caractérisé en ce que le corps dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un cinquième champ (5) de stockage d'une troisième information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données, de ladite fonction cryptographique et de ladite clé associée,

et en ce que ladite étape (92) de calcul par le module d'identification d'abonné dudit cryptogramme local comprend les étapes suivantes :

- le module d'identification d'abonné lit (94) ladite troisième information de localisation contenue dans le cinquième champ (5) dudit message amélioré ;
- le module d'identification d'abonné en déduit (95) l'emplacement de stockage de ladite fonction cryptographique et de ladite clé associée ;
- le module d'identification d'abonné calcule (96) ledit cryptogramme local, en utilisant ladite fonction cryptographique, ladite clé associée et au moins une partie

du contenu du second champ (4) dudit message amélioré.

19. Procédé selon les revendications 16 et 18, lesdits moyens de mémorisation de données du module d'identification d'abonné possédant une structure hiérarchique à au moins trois niveaux et comprenant au moins les trois types de fichiers suivants :

- 5 - fichier maître (MF), ou répertoire principal ;
- ) - fichier spécialisé (DF), ou répertoire secondaire placé sous ledit fichier maître ; )
- ) - fichier élémentaire (EF), placé sous un desdits fichiers spécialisés, dit fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent, ledit procédé étant caractérisé en ce qu'un fichier élémentaire système (EF SMS

10 System), propre à ladite application distante, contient une seconde information de localisation de l'emplacement de stockage, dans lesdits moyens de mémorisation de données du module d'identification d'abonné, de ladite valeur précédente du compteur de synchronisation, de ladite fonction cryptographique et de ladite clé associée,

15 en ce que ledit troisième champ (5) constitue également ledit cinquième champ, ladite première information de localisation constituant également ladite troisième information de localisation,

20 et en ce que ladite première information de localisation contenue dans ledit troisième champ (5) de stockage est un identificateur d'un fichier spécialisé (DF) ou d'un fichier maître (MF) auquel se rapporte ledit fichier élémentaire système (EF SMS System) selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

25 20. Procédé selon l'une quelconque des revendications 12 à 19, caractérisé en ce que le corps (2) dudit message amélioré transmis par le centre de service de messages à la station mobile comprend également un sixième champ (7) de stockage d'un total de contrôle, dit total de contrôle transmis, dont le calcul implique au moins en partie le contenu du premier champ (3) de stockage des commandes distantes,

et en ce que ledit procédé comprend également les étapes suivantes :

- le module d'identification d'abonné calcule (72) un total de contrôle local, en utilisant au moins en partie le contenu du premier champ (3) dudit message amélioré ;



- le module d'identification d'abonné compare (73) ledit total de contrôle transmis et ledit total de contrôle local, de façon que ledit message amélioré soit accepté si les totaux de contrôle transmis et local sont identiques, et refusé dans le cas contraire.

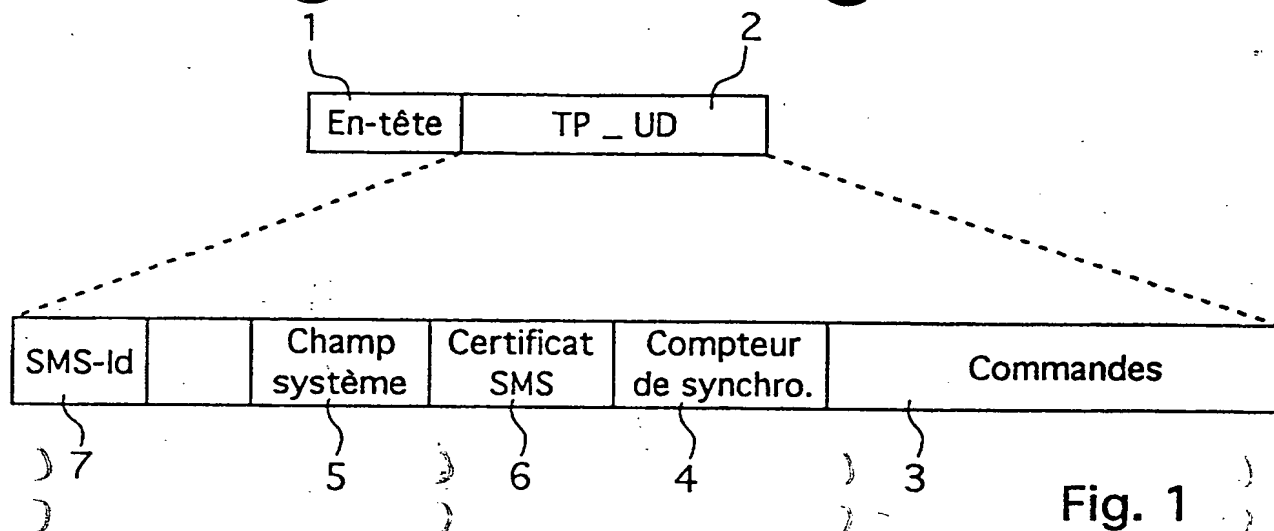


Fig. 1

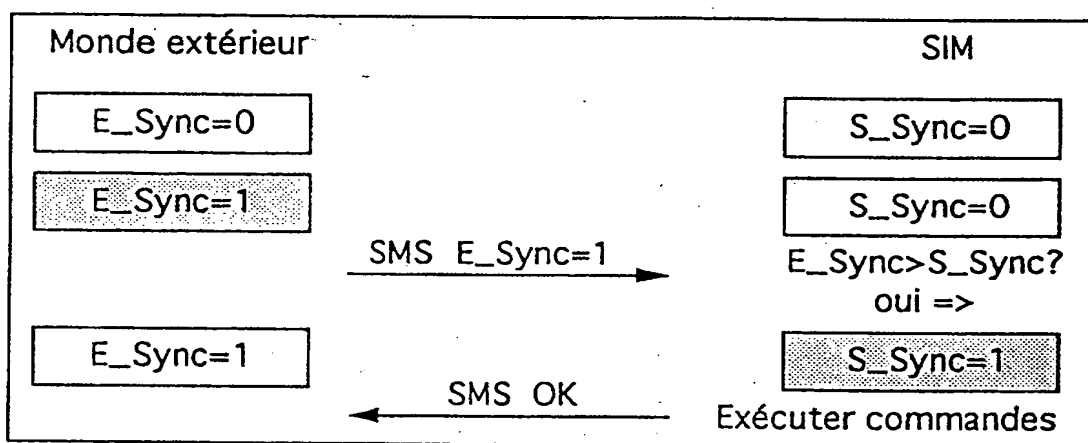


Fig. 2

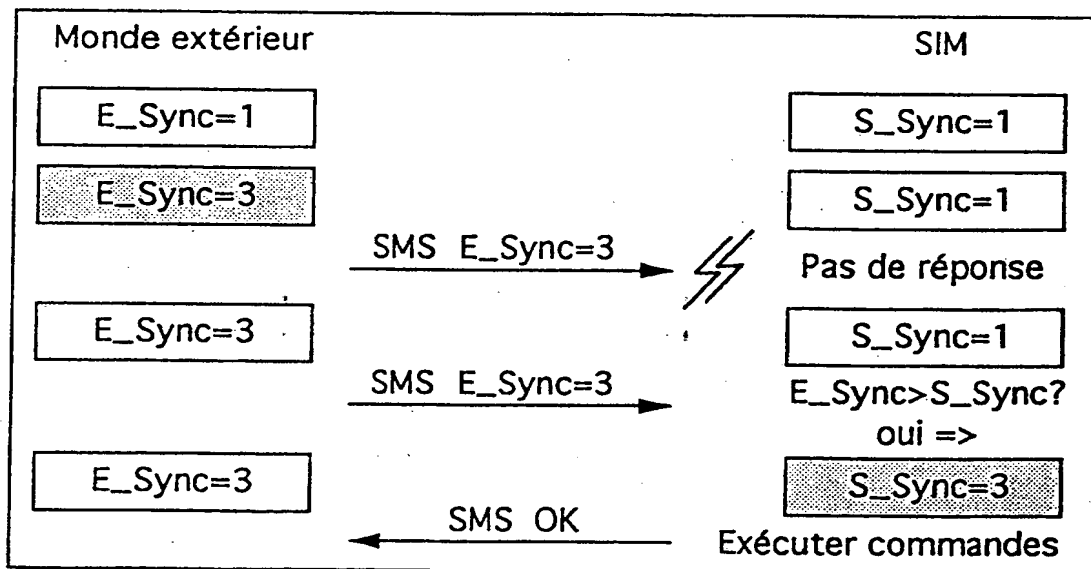


Fig. 3

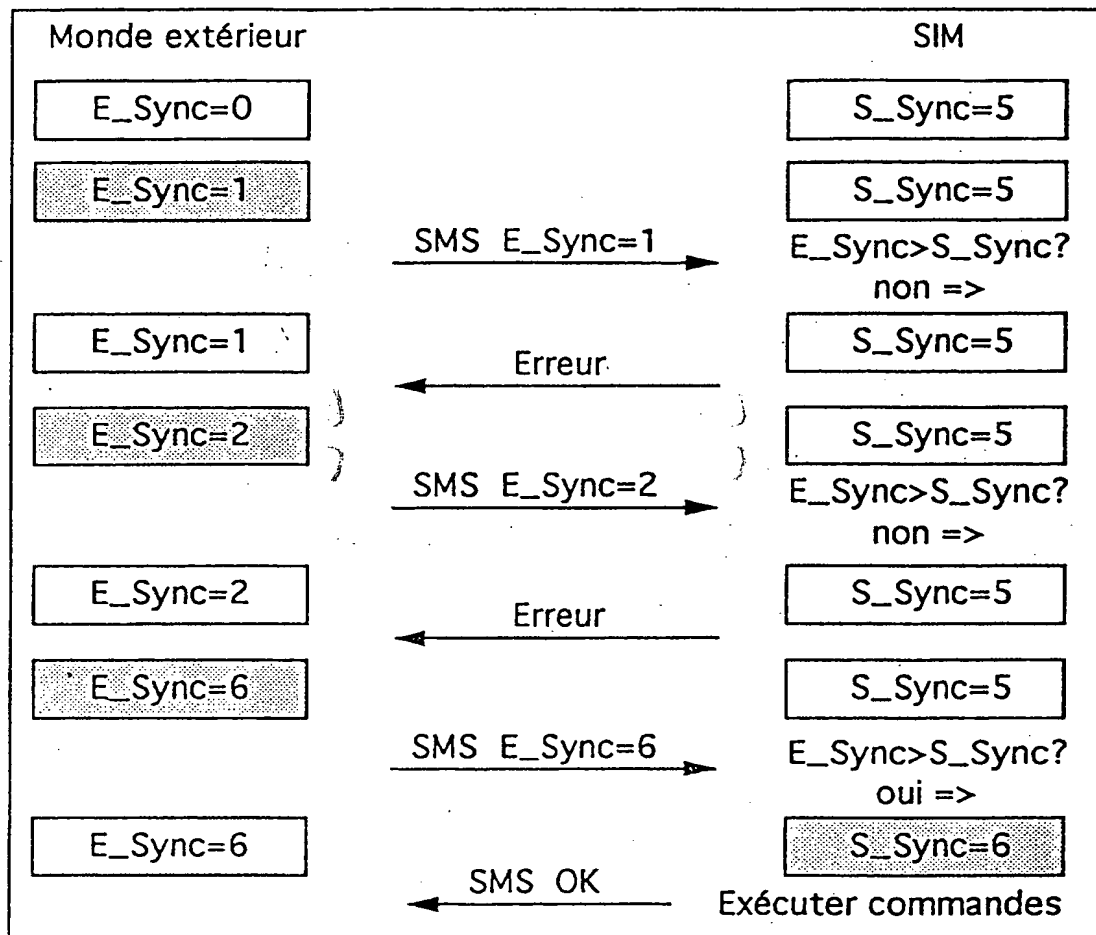


Fig. 4

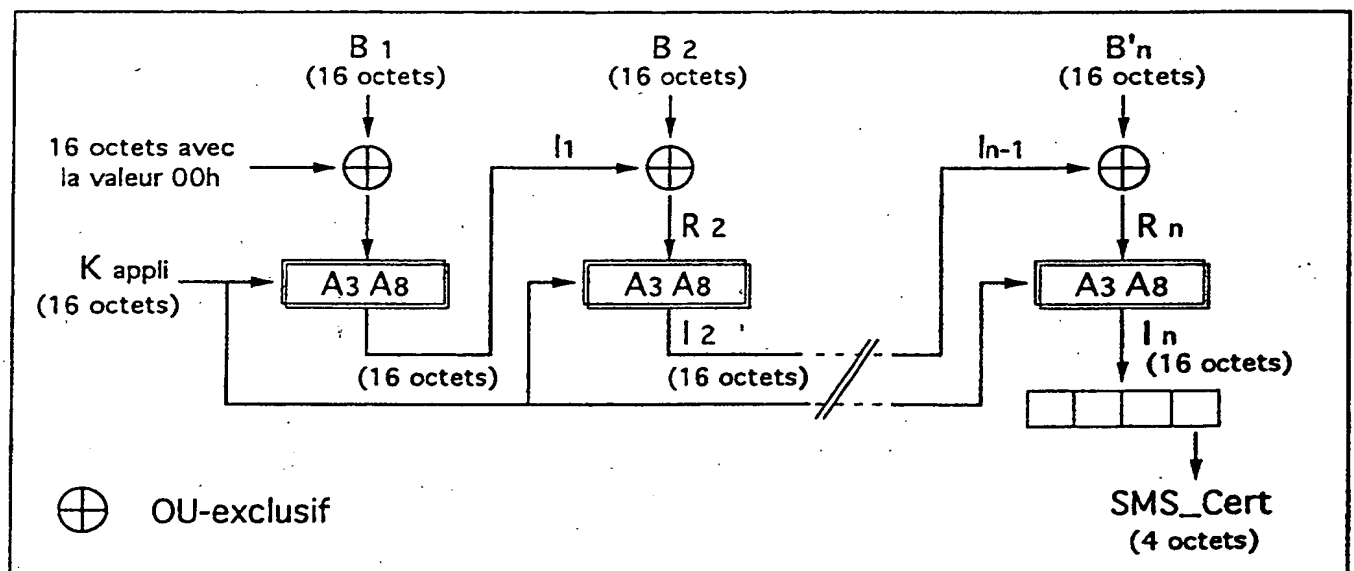


Fig. 5

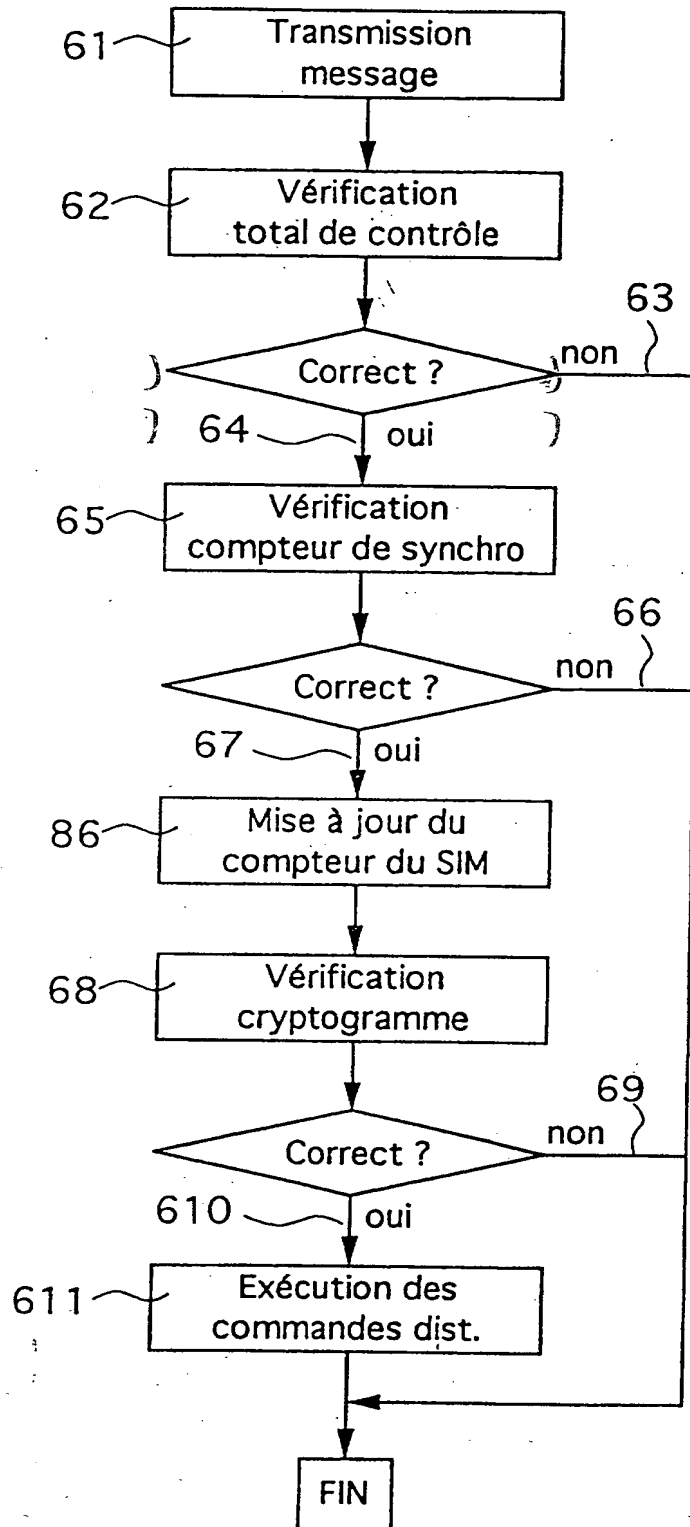


Fig. 6

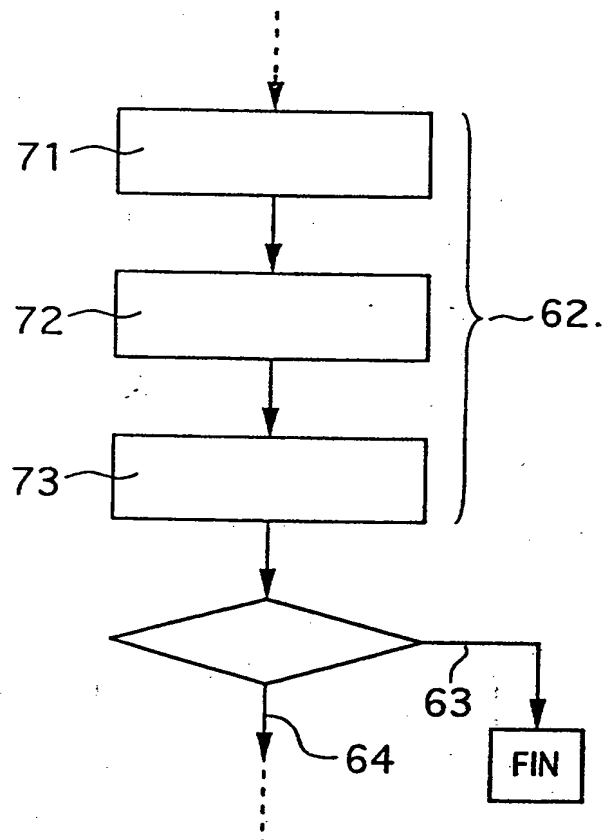
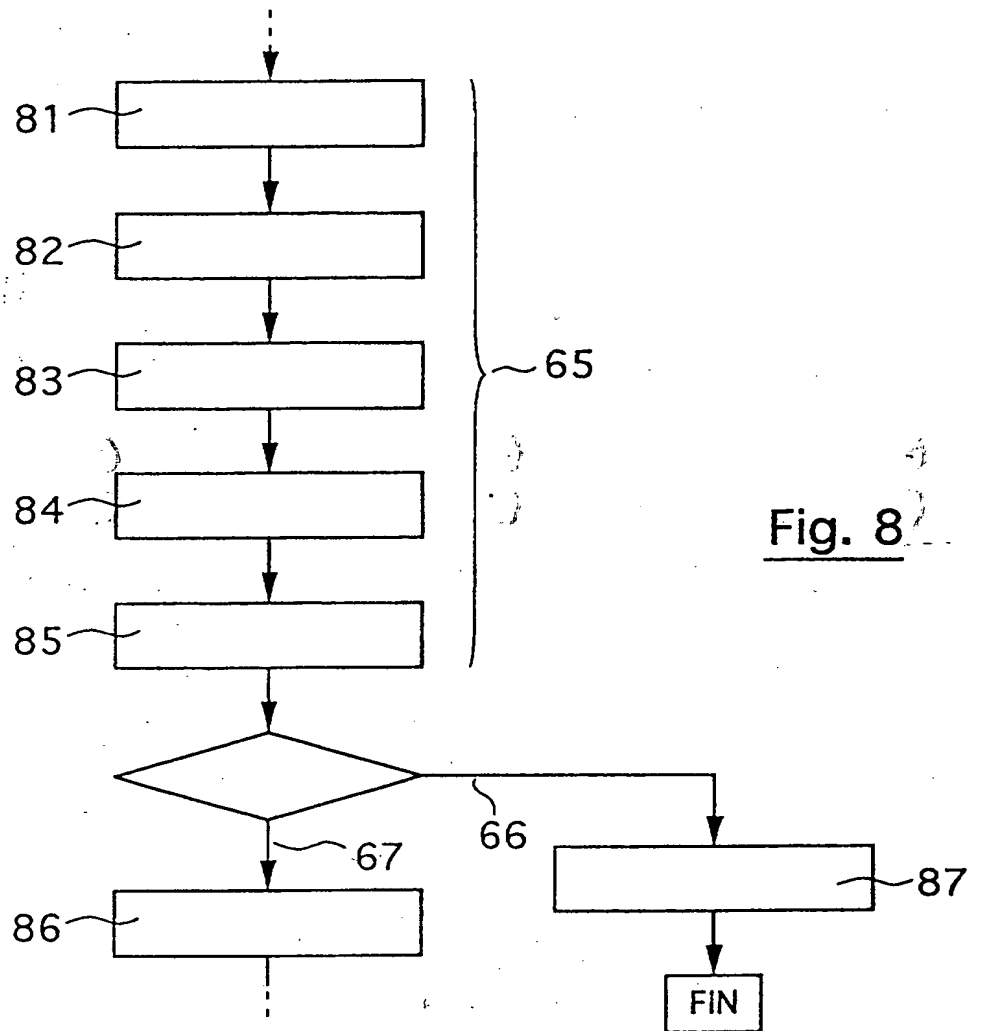
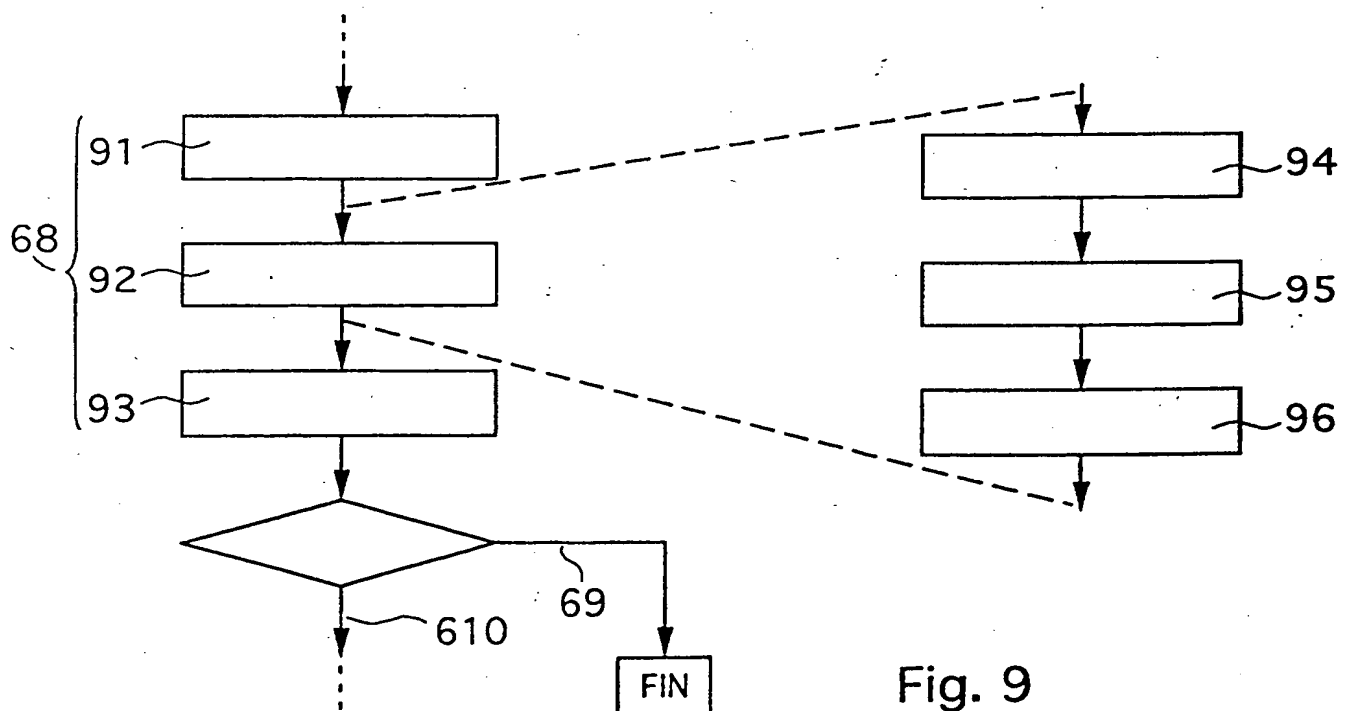


Fig. 7

Fig. 8Fig. 9

INSTITUT NATIONAL

RAPPORT DE RECHERCHE  
PRELIMINAIREde la  
PROPRIETE INDUSTRIELLEétabli sur la base des dernières revendications  
déposées avant le commencement de la rechercheFA 530703  
FR 9608906

| DOCUMENTS CONSIDERES COMME PERTINENTS  |   | Revendications<br>concernées<br>de la demande<br>examinée |
|--|---|---|
| Catégorie  | Citation du document avec indication, en cas de besoin,<br>des parties pertinentes  |   |
| X  | EP 0 689 368 A (PTT GENERALDIREKTION) 27<br>Décembre 1995<br><br>* colonne 3, ligne 29 - ligne 35 *<br>* colonne 4, ligne 1 - ligne 15 *<br>* colonne 5, ligne 7 - ligne 27 *<br>* colonne 5, ligne 32 - ligne 35 *<br>* colonne 8, ligne 33 - colonne 9, ligne<br>54 *<br>* colonne 10, ligne 26 - ligne 58 *<br>* colonne 12, ligne 3 - colonne 13, ligne<br>46 * | 1,4,7,<br>10,<br>12-14,<br>17,20                          |
| A  | US 5 517 187 A (BRUWER FREDERICK J ET AL)<br>14 Mai 1996<br>* colonne 3, ligne 9 - ligne 50 *<br>* colonne 3, ligne 64 - colonne 4, ligne<br>24 *<br>* colonne 4, ligne 34 - ligne 48 *<br>* colonne 8, ligne 7 - ligne 10 *<br>* colonne 9, ligne 21 - ligne 27 *<br>* colonne 10, ligne 14 - ligne 20 *   | 1,12-14   |
| A  | EP 0 644 513 A (AT & T CORP) 22 Mars 1995<br>* colonne 5, ligne 40 - colonne 6, ligne 5<br>*<br>* colonne 6, ligne 51 - colonne 9, ligne<br>14 *<br>* revendications 1,3,7,11 *   | 1,12  |
| A  | EP 0 562 890 A (HUTCHISON MICROTEL<br>LIMITED) 29 Septembre 1993<br>* page 4, ligne 30 - page 5, ligne 32 *<br>* page 6, ligne 10 - ligne 45 *<br><br>-/-   | 1,12  |
| Date d'achèvement de la recherche  |   | Examineur   |
| 14 Février 1997  |   | Gerling, J.C.J.   |
| <p><b>CATEGORIE DES DOCUMENTS CITES</b></p> <p>X : particulièrement pertinent à lui seul<br/>Y : particulièrement pertinent en combinaison avec un<br/>autre document de la même catégorie<br/>A : pertinent à l'encontre d'au moins une revendication<br/>ou arrière-plan technologique général<br/>O : divulgation non-écrite<br/>P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention<br/>E : document de brevet bénéficiant d'une date antérieure<br/>à la date de dépôt et qui n'a été publié qu'à cette date<br/>de dépôt ou qu'à une date postérieure.<br/>D : cité dans la demande<br/>L : cité pour d'autres raisons<br/>&amp; : membre de la même famille, document correspondant</p> |   |   |

EPO FORM 1503 03.82 (P04C13)



**THIS PAGE BLANK (USPTO)**